UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,962	12/11/2000	David Michael Kurn	20206-030 (P00-3014)	4932

7590 06/28/2004

Hewlett-Packard Company
Attn: Bill Streeter
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
NORRIS, TREMAYNE M	
ART UNIT	**PAPER NUMBER**
2137	6

DATE MAILED: 06/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/734,962	KURN ET AL.	
	Examiner	Art Unit	
	Tremayne M. Norris	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 25, 28-31 are objected to because of the following informalities:

With regards to claim 25, there are two different claims numbered "25", the first one should be numbered 24.

With regards to claims 28-31, sub-letters e,f, and g are repeated with different headings. The sub-letters need to be re-lettered.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 27-31 rejected under 35 U.S.C. 102(e) as being anticipated by Mitty et al (US pat 6,199,052).

Regarding claim 27, Mitty teaches a method for obtaining cryptographic credentials by an application running on a computer system, the method comprising the steps of

(a) providing a computer system having at least one server (col.9 lines 53-56);

(b) instantiating a Key Repository process on the computer system, the Key Repository process having a cryptographically protected database (col.4 lines 18-26; col.8 lines 34-40; col.9 lines 58-61);

(c) instantiating an application process on behalf of an end entity on the computer system, the end entity having credentials stored in the database (col.6 lines 24-33; col.11 lines 12-19);

(d) requesting the Key Repository process for the credentials of the end entity by the application process (col.2 lines 29-42); and

(e) if the Key Repository process authenticates the application process as having been pre-authorized to have the credentials (col.15 lines 6-20; col.19 lines 15-21), building an encrypted credentials file and providing the application process with the file and a password for the file (col.11 line 66 thru col.12 line 12).

Regarding claim 28, Mitty teaches instantiating a remote Key Repository process on a remote server (fig.1B; col.13 line 60 thru col.14 line 5).

Regarding claim 29, Mitty teaches instantiating a local agent on a remote server (fig.1B; col.13 line 60 thru col.14 line 5).

Regarding claim 30, Mitty teaches providing the Key Repository process with a remote agent interface; and

linking the remote Key Repository process on the remote server to the Key Repository process via the remote agent interface (fig.1B; col.13 line 60 thru col.14 line 5).

Regarding claim 31, Mitty teaches providing the Key Repository process with an agent interface; and

linking the local agent on the remote server to the Key Repository process via the agent interface (fig.1B; col.13 line 60 thru col.14 line 5).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1,3-22,25,26 rejected under 35 U.S.C. 103(a) as being unpatentable over Ober et al (US pat 6,307,936), and further in view of Mitty et al (US pat 6,199,052).

Regarding claim 1, Ober teaches a method for providing scalable security services, comprising:

instantiating at least one application on the computer system (col.3 lines 17-22; col.4 lines 53-54)); and

instantiating a Key Repository process on the computer system, the Key Repository process configured to manage sensitive information in a database on the computer system using at least one master key (col.1 line 49 thru col.2 line 15; col.10 lines 30-35).

What Mitty teaches that Ober does not teach is validating and recording authorizations of specific applications to access sensitive information in the database, wherein each of the at least one application is configured to query the Key Repository process for some or all of the sensitive information in the database (col.2 lines 29-55; col.10 lines 28-55)), and

in response to the query from a particular instance of the at least one application, provide to the particular instance of the at least one application the requested some or all of the sensitive information only if the Key Repository process authenticates the particular instance of the at least one application as being pre-authorized to receive the requested some or all of the sensitive information (col.15 lines 6-20; col.19 lines 15-21). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Ober's cryptographic key management scheme with Mitty's method of secure electronic transactions in order to provide a system that has privacy,

authentication of participants, and non-repudiation, and is able to prevent eavesdroppers from being able to determine that a given sender is communicating with a given recipient (Mitty col.2 lines 1-28).

Regarding claim 3, Ober and Mitty teach the method of claim 1, in addition Ober teaches the Key Repository process is a centralized repository process for the at least one master key, as well as passwords, enterprise policy and policy decisions, authorizations to use enterprise credentials and pre-authorization and authentication of the at least one application (col.6 lines 1-12; col.10 lines 30-35).

Regarding claim 4, Ober and Mitty teach the method of claim 1, in addition Ober teaches at least one master key is configured as an encryption key that maintains the integrity of and protects the sensitive information (col.10 lines 9-35).

Claim 5 is substantially equivalent to claim 1, therefore claim 5 is rejected because of similar rationale.

Regarding claim 6, Ober and Mitty teach the method of claim 5, in addition Ober teaches at least one master key maintains the integrity of and protects the sensitive information in the database (col.7 lines 21-24; col.7 lines 58-59).

Regarding claim 7, Ober and Mitty teach the method of claim 5, in addition Ober teaches at least one master key provides privacy protection to the sensitive information on the database (col.10 lines 9-35).

Regarding claim 8, Ober and Mitty teach the method of claim 5, in addition Ober teaches the sensitive information is a public key (col.4 lines 8-13).

Regarding claim 9, Ober and Mitty teach the method of claim 5, in addition Ober teaches the sensitive information is a secret (col.2 lines 58-60; col.3 lines 34-45).

Regarding claim 10, Ober and Mitty teach the method of claim 5, in addition Ober teaches the sensitive information is a private key (col.4 lines 14-23).

Regarding claim 11, Ober and Mitty teach the method of claim 5, in addition Ober teaches the sensitive information is a symmetric key (col.9 lines 30-38).

Regarding claim 12, Ober and Mitty teach the method of claim 5, in addition Mitty teaches the sensitive information is a certification authority certificate (col.4 line 62 thru col.5 line 25).

Regarding claim 13, Ober and Mitty teach the method of claim 5, in addition Ober teaches at least one master key are kept in physical memory (col.16 lines 40-51).

Regarding claims 14 and 15, examiner takes official notice that non-swappable physical memories are well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the invention to use non-swappable physical memory in order to allow the processor to focus on the tasks/jobs, such as tasks involving managing a key repository process and distributing sensitive information to authorized users, without wasting any allocated CPU time for swapping information in and out of memory.

Regarding claim 15, Ober and Mitty teach the method of claim 5, in addition Ober teaches the physical memory is protected (col.6 lines 10-12).

Regarding claim 16, examiner takes official notice that virtual memories are well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the invention to use virtual memories in order to allow a larger process to be executed by the CPU with a smaller amount of RAM.

Regarding claim 17, Ober and Mitty teach the method of claim 5, in addition Ober teaches at least one master key includes an integrity key configured to ensure the integrity of the sensitive information on the database (col.7 lines 21-23; col.7 lines 45-48).

Regarding claim 18, Ober and Mitty teach the method of claim 5, in addition Ober teaches at least one master key includes a protection key configured to protect the sensitive information on the database (col.10 lines 55-63).

Regarding claim 19, Ober and Mitty teach the method of claim 5, in addition Mitty teaches at least one application is a context-free server program (col.13 line 60 thru col.14 line 5).

Regarding claim 20, Ober and Mitty teach the method of claim 19, in addition Mitty teaches at least one application is configured to retain context information across one or more instantiations of the at least one application (col.7 lines 56-65; col.14 line 66 thru col.15 line 5).

Regarding claim 21, Ober and Mitty teach the method of claim 20, in addition Mitty teaches the context information includes sensitive data (col.7 lines 56-65).

Regarding claim 22, Ober and Mitty teach the method of claim 19, in addition Mitty teaches at least one application is configured to convey sensitive context information, by encrypting the information and then passing the information to a next instance of the at least one application (col.2 lines 29-55; col.11 line 60 thru col.12 line 12).

Regarding claim 25, Ober and Mitty teach the method of claim 9, in addition Mitty teaches the secret is protected by a password (col.4 lines 24-26).

Regarding claim 26, Ober and Mitty teach the method of claim 25, in addition Mitty teaches the secret can be updated in the absence of the password (col.2 lines 29-55).

6. Claims 2,23,25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ober and Mitty, and further in view of Price (US pat 6,662,299).

Regarding claim 2, Ober and Mitty teach the method of claim 1 but fail to teach at least one master key is divided into a predetermined number of portions each of which associated with a password, and wherein the sensitive information cannot be exposed without at least some or all of the predetermined number of passwords using a password-based private key encryption-decryption. Price teaches at least one master key is divided into a predetermined number of portions each of which associated with a password, and wherein the sensitive information cannot be exposed without at least some or all of the predetermined number of passwords using a password-based private key encryption-decryption (col.1 lines 55-59; col.2 lines 49-59). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Ober and Mitty's cryptographic key management scheme with Price's method for

reconstructing an encryption key in order to discard the need for maintaining backup copies of passwords for users that can severely compromise the computer system security due to un-trusted system administrators (Price col.1 lines 47-64).

Regarding claim 23, Ober and Mitty teach the system of claim 9, but fail to teach the secret is divided among a plurality of individuals. Price teaches the secret is divided among a plurality of individuals (col.1 lines 55-59; col.2 lines 49-59). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Ober and Mitty's cryptographic key management scheme with Price's method for reconstructing an encryption key in order to discard the need for maintaining backup copies of passwords for users that can severely compromise the computer system security due to un-trusted system administrators (Price col.1 lines 47-64).

Regarding claim 25, Ober, Mitty, and Price teach the system of claim 23, in addition Price teaches the integrity of the secret that is controlled by a first individual is increased by linking the secret to a second secret, the second secret is revealed only with the cooperation of all or a predetermined number of the plurality of individuals (col.1 lines 55-59; col.2 lines 49-59).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

June 17, 2004

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137